Our Ref.: 42390.P7947

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

A Stream Cipher Having A Combiner Function With Storage Based Shuffle Unit

Inventor(s): **Gary L. Graunke**
Carl M. Ellison

"Express Mail" mailing label number EL431684500US
Date of Deposit November 30, 1999
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Signature 11/30/99 Date

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP
12400 Wilshire Boulevard, 7th Floor
Los Angeles, California 90025
(503) 684-6200

"Express Mail" label number EL431684500US

A Stream Cipher Having A Combiner Function With Storage Based Shuffle Unit

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of cryptography. More specifically, the present invention relates to the robustness of stream ciphers.

2. Background Information

Crytographic ciphers can be broadly divided into block ciphers and stream ciphers. Block ciphers cipher a block of plain text into ciphered text by applying multiple successive rounds of transformation to the plain text, using a cipher key. An example of a block cipher is the well known DES cipher. Stream ciphers cipher a stream of plain data into ciphered data by combining the stream of plain data with a pseudo random sequence dynamically generated using a cipher key. An example of a stream cipher is the well known XPF/KPD cipher.

Most stream ciphers employ one or more linear feedback shift registers (LFSR). In various applications, it is desirable to employ multiple LFSRs to increase the robustness of a stream cipher. However, employment of multiple LFSRs requires employment of a combiner function to recombine the multiple data bits output by the LFSRs. Most combiner functions known in the art are inefficient in their real estate requirement for hardware implementations. Thus, a robust stream cipher with a more efficient combiner function is desired.

SUMMARY OF THE INVENTION

A stream cipher is provided with a first and a second data bit generators to generate in parallel a first and a second stream of data bits. The stream cipher is further provided with a combiner function having a shuffling unit including a storage structure to generate a pseudo random sequence, by combining the first stream of data bits with at least stochastically generated past values of the first stream of data bits, generated by using the second stream of data bits to stochastically operate the storage structure of the shuffle unit to memorize and reproduce the data bits of the first stream.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates an overview of the stream cipher of the present invention, in accordance with one embodiment;

Figure 2 illustrates a manner in which the LFSRs of **Fig. 1** are initialized, in accordance with one embodiment; and

Figures 3a-3b illustrate the shuffle unit of **Fig. 1** in further detail, in accordance with two embodiments.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention. However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating the stream cipher of the present invention, in accordance with one embodiment, is shown. As illustrated, stream cipher **100** includes a number of data bit generators **102** and a combiner function **104** coupled to each other as shown. Data bit generators **102** are initialized with an initial vector and a key. Upon initialization, data bit generators **102** are used to generate a number of streams of data bits, and the generated data bit streams are provided to combiner function **104**. Combiner function **104** in turn generates a pseudo random sequence using the provided data bit streams. More specifically, the sequence is generated by modifying one of the provided streams of data bits with at least stochastically selected past values of the stream. The

stochastic selection is effectuated based on the other streams. For the illustrated embodiment, in addition to the stochastically selected past values of the stream, the stream is further modified by the other streams.

As illustrated, data bit generators **102** may be formed with linear feedback shift registers (LFSR), complementary in number to the "capacity" of combiner function **104** (to be explained more fully later). For the illustrated embodiment, data bit generators **102** are formed with five linear feedback shift registers (LFSR) **112-120**. Combiner function **104** is formed with a storage unit based shuffling unit **122** and an XOR function **124**. Storage unit based shuffling unit **122** includes storage locations that can be selectively written into and read from. The number of storage locations included is complementary to the number of LFSRs employed to form data bit generators **102**. For the illustrated 5 LFSR embodiment, storage unit base shuffling unit **122** is equipped with at least 16 storage locations that can be selectively written into and read out of, using 4 of the 5 provided streams of data bits generated by LFSR **112-120**.

Upon initialization with the key and the initial vector, LFSR **112-120** is operated to generate five streams of data bits for combiner function **104**. Shuffling unit **122** shuffles one stream of data bits by stochastically storing the data bits into its storage locations, and at the same time, retrieving the previously stored data bits in the storage locations being written over, in accordance with the data bits of the remaining four streams. The retrieved past values are in turn used by XOR function **124** to modify the same stream of data bits, to generate the pseudo random sequence. For the illustrated embodiment, in addition to the retrieved past values of the stream, the XOR function also uses the other streams, streams generated by LFSR **114-120**, to modify the stream.

As will be appreciated by those skilled in the art, more or less LFSR and storage locations may be used to practice the present invention, as long as their capacities remain complementary to each other. In one embodiment, the five LFSR **112-120** are uneven in length. More specifically, their lengths are 31 bits, 29 bits, 27 bits, 25 bits and 23 bits. Additionally, each LFSR **112, 114, 116, 118** or **120** includes 8 taps. The tap positions are preferably spread out, in one embodiment, accordingly to the following position table:

LFSR	Tap positions
LFSR (31 bit)	31, 25, , 21, 17, 13, 11, 6, 1
LFSR (29 bit)	29, 24, 18, 17, 12, 9, 5, 1
LFSR (27 bit)	27, 23, 19, 15, 11, 7, 4, 1
LFSR (25 bit)	25, 21, 8, 14, 12, 8, 5, 1
LFSR (23 bit)	23, 18, 15, 12, 11, 8, 4, 1

Figure 2 illustrates a manner in which LFSR **112-120** are initialized with a key and an initial vector, in accordance with one embodiment. For the illustrated embodiment, the initial key is assumed to be 56 bits in size, whereas the initial vector is assumed to be 32 bits in size. Both the initial key as well as the as the initial vectors are sub-divided into 8-bit chunks, i.e. Key = K6 + K5 + K4 + K3 + K2 + K1 + K0, and Initial Vector (IV) = IV3 + IV2 + IV1 + IV0 (with K0 and IV0 being the least significant bits (LSB)). As illustrated, the 31-bit LFSR is initialized with K0, the complement of the LSB of K0, K5, K6 and a truncated K4, whereas the 29-bit LFSR is initialized with K1, IV3, K0, the complement of the LSB of K1, and a truncated K5. Similarly, the 27-bit LFSR is initialized with K2, IV0, the complement of the LSB of K2, K1 and a truncated K6, whereas the 25-bit LFSR is initialized with K3, IV1, the

complement of the LSB of K3, and K2. Finally, the 23-bit LFSR is initialized with K4, IV2, the complement of the LSB of K4, and a truncated K3. In alternate embodiments, keys and initial vectors of other lengths as well as other segmentation and loading strategies may be employed instead.

Figures 3a-3b illustrate shuffle unit **122** in further detail in accordance with two embodiments. For the embodiment of **Fig. 3a**, shuffle unit **122** includes memory unit **302** having 16 addressable memory locations **312**, data input port **314**, four write address pins **316,** four read address pins **318** and data output port **320**, thereby allowing the data bits streams generated by the LFSR **114-120** to stochastically control the writing of data bit stream generated by LFSR **112** into memory locations **312** as well as retrieving past values of the data stream previously stored in memory locations **312**. As earlier described, the past values are retrieved from the same storage locations being written into with new data values.

For the embodiment of **Fig. 3b**, shuffle unit **122** includes memory unit **352** having 16 memory locations **362**, 1 to n de-multiplexor **364**, and n to 1 multiplexor **366** (n being equal to 16 in this case), thereby also allowing the data bits streams generated by the LFSR **114-120** to stochastically control the writing of the data bit stream generated by LFSR **112** into memory locations **352** as well as retrieving past values of the data stream previously stored in memory locations **352**. Again, the past values are retrieved from the same storage locations being written into with new data values.

Epilogue

From the foregoing description, those skilled in the art will recognize that many other variations of the present invention are possible. Thus, the present

invention is not limited by the details described, instead, the present invention can be practiced with modifications and alterations within the spirit and scope of the appended claims.
